УДК 004.056

Коряк М.В.
Кіровоградський національний технічний університет

Аналіз існуючих загроз для СУБД MySQL та захист на прикладі MySQL Inject

MySQL - одна з найбільш розповсюджених СУБД. Її можна зустріти всюди, але найбільш часто вона використовується численними сайтами. Саме тому безпека бази даних - дуже важливе питання, оскільки зловмисник отримавши доступ до бази, може пошкодити не тільки ресурс, але і всю локальну мережу. В даній доповіді зібрана вся корисна інформація по злому і постексплуатації MySQL.

MySQL - це реляційна система управління базами даних, яка володіє різними двигунами зберігання даних: MyISAM, InnoDB, Archive і іншими.

Для того щоб виконати злом СУБД MySQL потрібно знайти що зламувати. Для цього використовується пошук SHODAN.

SHODAN — сервіс який дозволяє робити пошук по хостам і виводити інформацію про різноманітні сервіси на основі банерів відповідей (рис. 1).

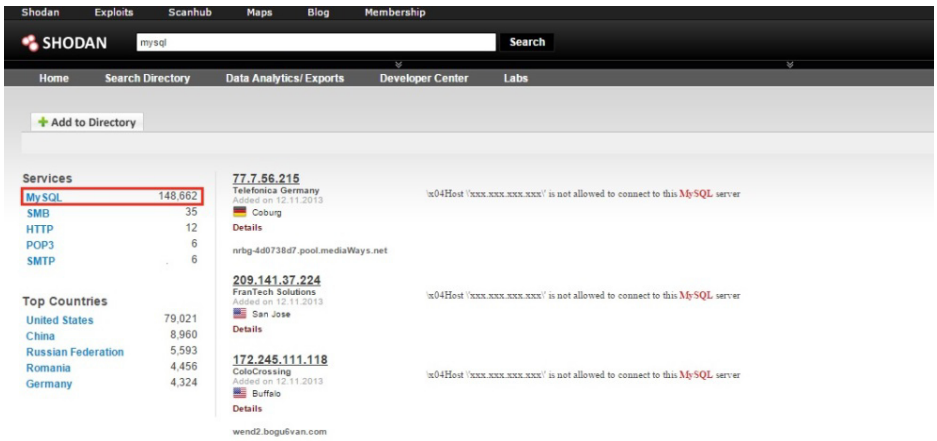

Рис 1. Результати пошуку MySQL в Shodan

Якщо жертва вже відома, потрібно просканувати його адресу на наявність відкритих портів. За стандартом MySQL використовує порт 3306, його потрібно знайти. В арсеналі кожного хакера повинен бути присутнім сканер Nmap.

Nmap ("Network Mapper") — утиліта з відкритим вихідним кодом для дослідження мережі та перевірки безпеки. Вона була розроблена для швидкого сканування великих мереж, хоча прекрасно справляється і з одиничними цілями. Nmap використовує необроблені IP пакети оригінальними способами, щоб визначити які хости доступні в мережі, які служби (назва програми і версію) вони пропонують, які операційні системи (і версії ОС) вони використовують, які типи пакетних фільтрів / брандмауерів використовуються і ще дюжини інших характеристик (рис. 2).

Для пошуку ін'єкцій існують різні способи, автоматично або вручну вставляти всюди лапки. До автоматичного, відноситься інструмент SQLmap — комп'ютерна програма, яка автоматизує процес пошуку і експлуатації SQL-ін'єкцій, і не просто знайде дірку в безпеці, а проексплуатує її в повній мірі.

Потрібно почати з самого простого - збору інформації. В Metasploit для цього служить сканер версій, який може сканувати цілий пул адрес.

Metasploit Project — проект сфери комп'ютерної безпеки, що надає інформацію про вразливості системи і допомагає у тестах на проникнення та розробці IDS.

Серед основних речей, котрі доводиться часто виконувати, звичайно, брутфорс — перевірка на слабкі або стандартні паролі користувачів.

Але перш ніж приступати до підбору паролів, можна провести атаку user enumeration (перерахунок користувачів). Її можна провести проти серверів версії 5.x, які підтримують старі механізми аутентифікації (CVE-2012-5615).

Рис 2. Nmap версії 4.53, самосканування

CVE-2012-2122 — Серйозна помилка безпеки в MariaDB і MySQL. Відповідно до Advisory, всі MariaDB і MySQL версії до 5.1.61, 5.2.11, 5.3.5, 5.5.22 вразливі. Цій помилці було присвоєно ідентифікатор CVE-2012-2122. Дана вразливість дозволяє віддаленим користувачам обходити аутентифікацію через неналежну перевірки значень, що повертаються.

Існує підтримка User-Defined Function (Введені користувачем певні функції). Вона підтримується досі в якості зовнішніх збережених функцій.9

User-Defined Function — (Введені користувачем певні функції) дані функції не просто комбінують різні SQL-оператори в якийсь певний запит, а ще й сильно розширюють функціональність самої бази.

Правила, дотримання яких гарантує захист від ін'єкцій:

- Дані потрібно підставляти в запит тільки через плейсхолдери

- ідентифікатори і ключові слова потрібно підставляти тільки з білого списку, прописаного в коді.

Плейсхолдер - це змінна, яка прописана в SQL-«скрипті» і не змінюється в залежності від даних, в той час як дані відправляються на сервер окремо від запиту, і ніколи з ним не перетинаються.

Експлойт, експлоїт — комп'ютерна програма, фрагмент програмного коду або послідовність команд, що використовують уразливості в програмному забезпеченні і приємним для проведення атаки на обчислювальну систему. Метою атаки може бути як захоплення контролю над системою (підвищення привілеїв), так і порушення її функціонування (DoS-атака).

Ескейпінг (mysql_real_escape_string) — екранує спеціальні символи в рядках для використання в виразах SQL.

Список використаних джерел

1. *Методи і засоби злому баз даних MySQL [Електронний ресурс]. – Режим доступу: https://xakep.ru/2015/04/16/195-mysql/*
2. *SQL Inject. Перевірка, злом, захист [Електронний ресурс]. – Режим доступу: https://habrahabr.ru/post/130826/*
3. *Захист від SQL Inject в PHP та MySQL Електронний ресурс]. – Режим доступу: https://habrahabr.ru/post/148701/*